Issue CSR as RabbitMQ Customer

SD Infrastructure

Exported on 10/21/2024

Table of Contents

You can use openssl to issue your private key and a CSR that should be send to Silkeborgdata for signing.

Example on using openssl

1 Create a openssl configuration.

Create a new folder that you use for the purpose

In the folder create a new file named openssl.cnf with content like this:

```
[ req ]
default_bits        = 2048
default_keyfile     = client.key
distinguished_name  = req_distinguished_name
req_extensions      = v3_req
prompt              = no

[ req_distinguished_name ]
C  = DK
ST = Midjylland
L  = Århus
O  = EG A/S
OU = SD
CN = sd-mox-9Z
emailAddress = jeeweb@sd.dk

[ v3_req ]
basicConstraints = CA:FALSE
keyUsage = digitalSignature, keyEncipherment
extendedKeyUsage = clientAuth
```

Replace values in the *req_distinguished_name* section with values relevant for your request

2 Issue private key and CSR

Now it's time to issue the private key and the CSR:

```
openssl genpkey -algorithm RSA -out client.key -pkeyopt rsa_keygen_bits:2048

# Generate a CSR
openssl req -new -key client.key -out client.csr -config openssl.cnf
```

Send the generated *client.csr* file to Silkeborgdata for signing. You will receive a signed certificate that should be used to create a pkcs12 file once the CSR has been signed

3 Create pkcs12 file with signed certificate

Once you have received a signed certificate you can create a pkcs12 file that you can use for client authentication (mTLS)

```
openssl pkcs12 -export -out cert.pfx -inkey client.key -in signed-certificate.cer
-CAfile cafile.pem
```